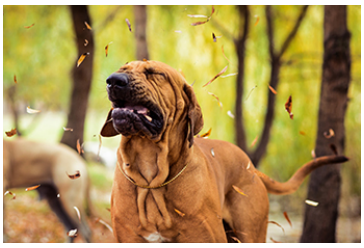

New Cyber Risks With COVID-19

cyber security pandemic

Summary: A recent report shares the newest cyber risks related to COVID-19. We give you the abbreviated version so you are prepared.

Did you know dogs sneeze to show they are play-fighting? So, no need to worry about your pooch, if you hear him sneeze.

Unfortunately, one thing you still need to worry about is cybercriminals. COVID-19 has provided a major opportunity for these bandits. Many of you have likely been hearing this, so we wanted to share the latest information.

According to "The Cyber Threat Impact of COVID-19 to Global Business," from cybersecurity firm IntSights, cybercrime has ramped up significantly with the outbreak. From targeted phishing efforts to phony coronavirus mobile apps, malware, and more, cybercriminals are taking full advantage of every opportunity.

Phony Apps. With people eager to monitor the impact of COVID-19, mobile apps that provide real-time information have sprung up. Unfortunately, not all of them are legitimate. Cybercriminals have created an array of phony coronavirus apps that appear to track the virus, but are just a way to infiltrate devices. Some examples of fake apps include CoronaVirus 1.6 APK and Coronavirus Live. Inform your customers and staff.

As more people than before are embracing mobile apps (not only for COVID-19 information but for banking too), community financial institutions should be on the **lookout for any apps impersonating your own offerings**. Remember, this relates not only to your own app but also to any partnership apps where you may have an API connection. Helping customers download your app for the first time with detailed information on your website or through your call center could help stem any issues or confusion.

Phishing Domains. Sadly, the uncertainty around COVID-19 has allowed cybercriminals to take full advantage of the desire for the latest coronavirus information. According to IntSight's findings, the number of registered domains including the words "COVID" or "corona" exceeded 38k at the end of March 2020, compared with only 190 domains using those words in 2019. As people eagerly search for new websites, these thieves stand ready to trick them, so be sure to widely communicate this danger too.

Tricky Malware. Cybercriminals are being aggressive in their phishing emails these days too, impersonating organizations such as the Department of Homeland Security. They send emails that claim to have important information regarding COVID-19 and contain links or downloads that infect a user's device with malware. One type of malware that we found especially alarming is one that mimics the Johns Hopkins' legitimate COVID-19 tracker and redirects the victim to the perpetrator's site. While many people know not to click on links within unsolicited emails, cybercriminals are counting on the fact that many people are acting on fear, not on common sense.

Because of all of this, it is incredibly important to continue reminding your employees and customers about the dangers of phishing and malware. You should also ensure all your technology (hardware and software) is well

monitored and tested regularly, including the necessary updates as new risks appear -- and there are always new risks.

<B>WEBINAR:</B> COVID-19 AND YOUR LOAN PORTFOLIO

The current crisis and uncertain times ahead mean needing a different approach to managing your loan portfolio. Join us on Thursday, May 14th at 9 a.m. PT, as we discuss how to incorporate the impact of COVID-19 into your loan management process.